Consejo de Transparencia
y Protección de Datos
de Andalucía

ANÁLISIS SOBRE BRECHAS DE SEGURIDAD Y RECLAMACIONES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN EL SECTOR PÚBLICO ANDALUZ

2019-2022

CONTENIDO

1. RESUMEN EJECUTIVO

El Consejo de Transparencia y Protección de Datos de Andalucía (en adelante, el Consejo) asumió sus funciones en materia de protección de datos personales el 1 de octubre de 2019. Uno de sus cometidos, según lo establecido en el Reglamento General de Protección de Datos (RGPD), es promover la sensibilización de los responsables y encargados del tratamiento acerca de sus obligaciones en virtud de dicho Reglamento.

A lo largo de estos años, hemos acumulado una valiosa experiencia que puede resultar de gran utilidad para los responsables y encargados de tratamiento en su esfuerzo por mejorar la protección efectiva de los derechos y libertades de las personas afectadas.

En este documento, se analizan las principales causas de las brechas de seguridad y de los motivos que provocaron reclamaciones por presunta vulneración de la normativa. El factor principal que desencadena las brechas es el ciberincidente, que incluye casos de 'hacking', 'malware' o 'phishing', seguido por el robo o pérdida de dispositivos electrónicos. En cuanto a las reclamaciones, el motivo más común es la comunicación o publicación indebida de datos personales.

Para abordar estas problemáticas, el Consejo ha desarrollado una lista de medidas prácticas con la consideración de que no impliquen un desembolso económico importante, facilitando así su implementación. En cualquier caso, más allá de la necesidad de medidas de seguridad ampliamente conocidas, la principal conclusión que se destaca es la importancia de la formación y concienciación en materia de protección de datos, así como la necesidad de contar con protocolos y procedimientos de actuación. Estas medidas son accesibles para todas las organizaciones, independientemente de su tamaño o recursos disponibles.

2. INTRODUCCIÓN Y ALCANCE

El Consejo es la autoridad independiente de control en materia de transparencia y protección de datos de la Comunidad Autónoma de Andalucía, creado por la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía.

El Consejo asumió las funciones que tiene atribuidas en materia de protección de datos personales el día 1 de octubre de 2019. Sus competencias en dicha materia abarcan los tratamientos de los que sean responsables las instituciones autonómicas de Andalucía, la Administración de la Junta de Andalucía, la Administración Local en Andalucía y otras entidades dependientes de cualquiera de ellas, así como por las universidades del sistema universitario andaluz.

Una de las funciones atribuidas al Consejo en virtud del Reglamento General de Protección de Datos (RGPD) es la de promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del Reglamento.

Por otra parte, tal y como se recoge en la Exposición de motivos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD): "*Es preciso tener en cuenta que la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan*".

El presente documento tiene como objetivo fomentar el cumplimiento de dicho principio de responsabilidad activa entre los responsables y encargados de tratamiento. Compartimos la experiencia acumulada durante estos años en el Consejo al objeto de asistirles en la mejora de la protección efectiva de los derechos y libertades de los interesados y en el despliegue de entornos de tratamientos más seguros y respetuosos con el derecho fundamental de las personas a la protección de datos.

De manera más concreta, entre las funciones que desarrolla el Consejo, están la de recepcionar y analizar las notificaciones de los responsables de tratamiento sobre violaciones de seguridad de datos personales así como la de resolver las reclamaciones presentadas por incumplimiento de la normativa.

Según el RGPD, se considera una *violación de la seguridad de los datos personales* (en adelante brecha de datos personales) toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Cualquier organización que trate datos personales se encuentra expuesta a sufrir una brecha de datos personales que pueda repercutir en los derechos y libertades de las personas físicas, y por tanto está obligada a preverlas y gestionarlas adecuadamente.[1]

Por otra parte, cuando las personas consideran que se ha producido una vulneración de la normativa en materia de protección de datos personales por parte del responsable de tratamiento, pueden interponer una reclamación ante la autoridad de control competente. En el caso de responsables pertenecientes al sector público andaluz resulta ser el Consejo. Las reclamaciones presentadas ante el Consejo pueden clasificarse en dos grupos. El primero referido a la vulneración del ejercicio de los derechos en materia de protección de datos contemplados en los artículos 15 al 22 del RGPD. Estos derechos se ejercen ante los responsables del tratamiento, que han de atender la solicitud presentada con carácter general en el plazo de un mes (sin perjuicio de posibles ampliaciones de plazo contempladas en la norma). Si no se ha obtenido respuesta o no se está de acuerdo con la misma, es posible dirigirse al Consejo para efectuar una reclamación relativa a la presunta vulneración de tus derechos.

El segundo grupo se refiere a cualquier otro tipo de vulneración de la normativa en materia de protección de datos personales. Serán las reclamaciones contempladas en este segundo grupo las analizadas, debido a la diversidad de posibles causas y la oportunidad de realizar recomendaciones concretas para minimizar su ocurrencia.

A lo largo de estos casi 4 años de experiencia, el Consejo ha acumulado una importante información sobre los principales motivos por los que o bien se producen brechas de seguridad o bien una persona considera vulnerado su derecho fundamental a la protección de datos (recordemos que se han exceptuado del análisis las reclamaciones motivadas por vulneraciones producidas en el ejercicio de los derechos).

Así, analizando estos motivos, el Consejo ha elaborado una lista de recomendaciones de carácter eminentemente práctico que ayuden a impedir que estas situaciones vuelvan a producirse. La puesta en práctica de estas medidas u otras similares ayudarán sin duda a mejorar la protección de los derechos y libertades de las personas físicas.

1 https://www.aepd.es/es/documento/guia-brechas-seguridad.pdf

2.1 Enfoque del análisis de las reclamaciones

Al respecto de las reclamaciones analizadas es importante destacar que hemos analizado los motivos por los que una persona considera que sus derechos no han sido respetados, independientemente si realmente lo fueron o no.

Se trata de la realización de un ejercicio de análisis partiendo de la perspectiva establecida en el Considerando 7 del RGPD, uno de cuyos objetivos es establecer un marco más sólido y coherente para la protección de datos que permita generar la confianza necesaria para el desarrollo de la economía digital.

Por tanto, en lo que respecta a la información sobre reclamaciones, se han analizado los motivos aducidos por las personas en sus reclamaciones. No sólo se analizan las causas de las brechas o de los incumplimientos, sino también la percepción (a través de las reclamaciones) de las personas cuyos datos son tratados.

El documento analiza, al respecto de las reclamaciones, la potencial vulneración de sus derechos que la ciudadanía considera haber experimentado, sin que necesariamente implique que así haya sido.

3. CAUSAS MÁS FRECUENTES DE LAS BRECHAS

Se han analizado un total de 111 brechas de seguridad. Tras la calificación de cada una de las brechas según el tipo de incidente que las causó, se procede a destacar únicamente los tipos que causan el mayor número de brechas. En concreto, los siguientes 4 tipos aglutinan el 80% de todas las brechas de datos personales registradas.

TIPO DE INCIDENTE	NÚMERO
CIBERINCIDENTE: HACKING, MALWARE O PHISHING	**50**
DISPOSITIVO PERDIDO, ROBADO O DESECHADO	**15**
DATOS ENVIADOS / MOSTRADOS POR ERROR (POSTAL O ELECTRÓNICAMENTE)	**13**
PUBLICACIÓN INDEBIDA	**10**

Tabla 1. Tipos incidentes que causan más brechas

Se procede seguidamente a describir y analizar cada uno de los tipos de incidentes desde la perspectiva de la protección de datos personales.

Ciberincidente: '*Hacking*', '*malware*' o '*phising*'

Es la causa que más brechas genera, lo que resulta coincidente con la información que publican el resto de autoridades de control tanto nacionales como internacionales. Se trata de incidentes generados por un actor externo a la organización cuyo objetivo es obtener un beneficio ilícito mediante el daño causado. Las consecuencias de estos ataques puede conllevar el acceso a información, su exfiltración (transferir información de manera no autorizada desde un sistema informático a un lugar externo) y el cifrado ilícito de la misma para impedir su uso. En particular, destaca el número y el impacto de los ataques mediante llamados '*ransomware*', ya que además de las consecuencias mencionadas, suele provocar interrupción de los servicios durante periodos de tiempo considerables.

Los ataques de *'ransomware'* vienen en muchos casos precedidos de ataques de '*phising*' (intento de hacerse pasar por una persona o entidad de confianza para que la víctima realice alguna acción que no debería realizar) mediante correo electrónico cuyo objetivo es el robo de credenciales de acceso a equipos como paso previo a los mismos. Según las últimas publicaciones, el 99,9% de las vulnerabilidades explotadas se utilizaron transcu-

rrido más de un año desde que fueran descubiertas y publicadas, por tanto con una actualización de seguridad disponible y habitualmente con tiempo suficiente para ser instaladas.

En ocasiones, se observa un cierto desconocimiento por parte del responsable del tratamiento, tanto de las causas del incidente como de las medidas de seguridad desplegadas con carácter previo a la brecha, así como las adoptadas con posterioridad a la misma. Son casos, habitualmente, en los que a través de un contrato o de cualquier otro instrumento jurídico, el tratamiento se realiza por cuenta de un encargado de tratamiento. Esta circunstancia, perfectamente compatible con la normativa vigente de protección de datos, no exime de la obligación del responsable, que es quien debe velar por garantizar la seguridad de los tratamientos y debe elegir únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del RGPD y garantice la protección de los derechos del interesado.

Dispositivo perdido, robado o desechado

Este incidente se ha reportado mayoritariamente debido al robo de dispositivos, que se produce en multitud de circunstancias y ubicaciones, siendo menores los casos reportados de pérdida.

En particular, destacan los portátiles que solían contener importantes cantidades de datos personales relacionados con la labor profesional de las personas usuarias de los mismos. También se han producido robos o pérdida de documentación en papel con datos personales de categorías especiales y de memorias de almacenamiento (pen-drive).

Datos enviados / mostrados por error (postal o electrónicamente)

Se trata de un tipo de incidente causado por errores humanos, habitualmente empleando herramientas de correo electrónico en los que se envía información a destinatarios incorrectos.

Destacan los casos en los que se emplean listas de distribución que contienen un elevado número de direcciones de correo electrónico, ya que un único error (basta con incluir la dirección de la lista) es suficiente para comunicar los datos a un elevado número de personas.

Publicación / comunicación indebida

Se produce cuando se publican en algún medio o se comunican datos personales de forma indebida y extensa. Puede entenderse como una generalización del caso anterior. En la mayoría de los casos se trata de errores humanos (por ejemplo, publicar el DNI completo en un boletín oficial o listar datos identificativos completos de los participantes de procesos selectivos) o errores técnicos (la configuración errónea de una aplicación permite acceder a información de otros clientes, pacientes, estudiantes, otros empleados, etc.).

4. CAUSAS MÁS FRECUENTES DE LAS RECLAMACIONES

Se han analizado un total de 421 reclamaciones. Tras la calificación de cada una ellas según el motivo que provocó la reclamación, se procede a destacar únicamente aquellos que causan el mayor número de reclamaciones presentadas ante el Consejo.

En concreto, los siguientes 9 motivos abarcan el 75% de todas las reclamaciones presentadas (excluyendo las presentadas por vulneración del ejercicio de derechos) registradas.

MOTIVO	NÚMERO
COMUNICACIÓN INDEBIDA DE DATOS	97
DIFUSIÓN O PUBLICACIÓN INDEBIDA DE DATOS	73
MEDIDAS TÉCNICAS	24
ACCESO INDEBIDO A HISTORIA CLÍNICA	23
VIDEOVIGILANCIA INCUMPLIENDO NORMATIVA	22
TRATAMIENTO SIN EL CONSENTIMIENTO DEBIDO	21
CARENCIA DPD	21
TRATAMIENTO INDEBIDO DE DATOS	20
USO DE DATOS PARA FINALIDADES INCOMPATIBLES	15

Tabla 2. Motivos que originan las reclamaciones más frecuentes

Se procede seguidamente a describir y analizar cada uno de los motivos desde la perspectiva de la protección de datos.

Comunicación indebida de datos y difusión o publicación indebida de datos

La comunicación (a un número concreto de personas) junto con la difusión (a un número indeterminado de personas, por ejemplo mediante la publicación en internet) de datos personales sin una adecuada base legitimadora o sin cumplir con otros principios establecidos en el RGPD representan el principal motivo de las reclamaciones recibidas en el Consejo. Recordemos que dicho motivo también figura entre los principales tipos de incidentes de las brechas analizadas.

Es frecuente que la reclamación esté relacionada con el principio de "minimización de datos", produciéndose una comunicación o difusión de datos personales en la que el reclamante considera que no son estrictamente necesarios para la finalidad del tratamiento. En otros casos, el reclamante denuncia directamente la falta de consentimiento, en cuyo caso será necesario analizar primero si existe otra base legitimadora del tratamiento y en su caso, si pudiera haberse producido algún otro incumplimiento de los principios general del RGPD.

Como medios habituales empleados en estos casos, destacan las páginas webs, el correo electrónico, los sistemas de mensajería instantánea y los medios de comunicación, siendo los ayuntamientos los que más casos presentan. Los contenidos son muy diversos incluyendo fotografías, vídeos, audios o mensajes privados de sistemas de mensajería instantánea, informes médicos, resoluciones judiciales, denuncias y datos de menores en el ámbito educativo.

Falta de medidas técnicas

Se contemplan tanto situaciones en las que considera que no existían medidas técnicas adecuadas o si las había, no resultaron eficaces para garantizar un nivel de seguridad adecuado.

Habitualmente nos encontramos ante reclamaciones por lo que se percibe como quiebras de la dimensión de confidencialidad. La consecuencia más habitual reprochada por los reclamantes es el acceso no autorizado a datos personales. Cuando efectivamente se hayan producido dichos incidentes, debe realizarse la misma consideración que en el caso de las brechas causadas por ciberincidentes.

Acceso indebido a historia clínica

Se producen en el ámbito sanitario. En concreto, en situaciones en los que las personas consideran que su derecho a la protección de datos personales se ha visto vulnerado por un acceso a su historia clínica que no debería haberse producido. Dado que se trata de una apreciación particular y no un hecho jurídico constatado, la reclamación se traslada al responsable del tratamiento que, con carácter general, inicia procedimiento de información reservada para la investigación de los hechos. Del resultado de dicha investigación puede concluirse que el acceso a la historia clinica se ha efectuado correctamente, justificando la relación asistencial de éste con la persona reclamante o el motivo lícito que lo permite o bien finalizar corroborando que efectivamente ha tenido lugar un acceso indebido a la historia clínica. En este último supuesto, la causa subyacente puede ser la falta de implantación de medidas técnicas y organizativas por parte del órgano responsable para garantizar la confidencialidad de la documentación que contiene datos de carácter personal (historia clínica) y para evitar el posible acceso a datos personales por parte terceros, lo que conlleva que dicho personal no conozca las condiciones y limitaciones a que está sometido dicho acceso ni las limitaciones que establece la normativa de protección de datos debido. También puede ocurrir que el personal sí que reciba instrucciones en materia de protección de datos y conozca las condiciones a qué está sometido por esta normativa pero acceda a los datos personales de la historia clínica desatendiendo las medidas establecidas por el órgano responsable, sin la legitimación necesaria.

Por tanto, en los casos en los que efectivamente se hubiese producido un acceso indebido a la historia clínica, además de la incoación de un procedimiento sancionador en materia de protección de datos, pueden derivarse responsabilidades administrativas, e incluso penales para las personas que realizan el acceso indebido.

Videovigilancia incumpliendo normativa

El uso cada vez más frecuente de la videovigilancia es causa de preocupación social dado lo invasivo para la espera privada que estos tratamientos pueden resultar.

Lo más frecuente es que se reclame que este tratamiento excede los límites permitidos o que se realiza sin la información debida. Se presentan en todos los ámbitos y contextos: laboral, educativo, zonas públicas así como en entornos privados. En este último caso, las reclamaciones son trasladadas a la AEPD, por ser la competente en dicho ámbito.

Tratamiento indebido de datos o sin el consentimiento debido

Se abordan principalmente situaciones en las que se reclama que o bien no existía una base legitimadora de las establecidas en el artículo 6 RGPD (o artículo 9 RGPD, para categorías especiales) o bien no se proporcionó la información mínima requerida según los artículos 13 y 14 RGPD a los interesados.

Nuevamente, vuelve a destacar dentro de esta categoría la percepción de los reclamantes de que se hayan realizado tratamientos que debían contar con el consentimiento del interesado y éste no fue recabado. Sin embargo, debe tenerse en cuenta que en el ámbito de las Administraciones Públicas, aunque existen supuestos excepcionales en los que efectivamente debería haberse solicitado el consentimiento del afectado, con carácter general las condiciones de licitud serán el cumplimiento de una obligación legal o el ejercicio de poderes públicos. Por tanto, para poder concluir sobre la responsabilidad de un órgano reclamado en relación con los hechos denunciados, habrá que determinar si la operación de tratamiento se ha realizado de acuerdo con alguna de las condiciones de licitud mencionadas y, además, si los datos tuvieran el carácter de categoría especial de datos (por ejemplo datos de salud, biométricos,etc.), habrá que verificar también si se da alguna de las circunstancias contempladas en el artículo 9.2 RGPD y que permiten levantar la prohibición establecida, con carácter general, para el tratamiento de dichas categorías de datos.

Carencia de Delegado de Protección de Datos

Todo organismo público tiene la obligación de designar un Delegado de Protección de Datos (DPD). Se trata de una figura clave en la organización como impulsor del cumplimiento del principio de responsabilidad proactiva, informando y asesorando al responsable del tratamiento y promoviendo una cultura de privacidad dentro de la organización, formando a los empleados y fomentando buenas prácticas en el manejo de la información personal.

La ausencia de un (DPD) en la organización puede revelar un problema respecto a la protección de datos personales y generar incumplimientos y vulneraciones de los derechos y libertades de las personas, muchos de los cuales se ven reflejados en las brechas y las reclamaciones analizadas en este documento.

Uso de datos para finalidades incompatibles

Los datos personales recogidos para una finalidad (que deberá ser determinada, explícita y legítima) no pueden ser tratados posteriormente para otra finalidad incompatible, de acuerdo con lo dispuesto en el artículo 5.1.b del RGPD. En esta categoría, se contemplan los casos en los que una vez las personas han proporcionado sus datos, estas estiman que los mismos se han usado para fines que consideran lesivos para sus derechos.

5. RECOMENDACIONES

Tras el análisis de los principales causas origen de las brechas de seguridad de los datos personales así como de las reclamaciones por incumplimientos en materia de protección de datos, se procede a realizar una serie de recomendaciones concretas que pueden contribuir a minimizar la probabilidad de ocurrencia en las organizaciones.

El "riesgo cero" no existe y por tanto es imposible plantear unas recomendaciones que descarten por completo una posible materialización de un riesgo concreto. No obstante, aplicar de modo diligente las siguientes recomendaciones sí contribuirá a disminuir la probabilidad tanto incurrir en incumplimientos en la materia como de ocurrencia de una brecha de seguridad de datos personales.

Finalmente, debe indicarse que estas recomendaciones no representan una lista exhaustiva de las medidas técnicas y organizativas necesarias para cumplir con las obligaciones establecidas en el RGPD.

5.1 Ciberincidente: "*Hacking*", "*malware*" o "*phising*" y medidas técnicas

El marco de referencia para hacer frente a las brechas o las reclamaciones causadas por estos motivos es el artículo 32 RGPD que establece la obligación de garantizar un nivel de seguridad adecuado al riesgo de los tratamientos. De forma coherente con dicho artículo, para el sector público la LOPDGDD establece la obligatoriedad de aplicar las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad (ENS).

Por tanto, con carácter general, la primera y mejor recomendación es obtener la certificación de conformidad con el ENS, así como su revisión periódica. Para las entidades locales, dada la dificultad que ello podría suponer, resulta de especial interés la iniciativa "Marco de certificación específico con el ENS para entidades locales", desarrollada por el Centro Criptológico Nacional, con especial atención en conseguir una adecuación al ENS

lo más posibilista y pragmática posible. Puede encontrarse más información en https://ens.ccn.cni.es/es/entidades-locales.

Seguidamente, con independencia de lo anterior, se proponen una serie de medidas concretas:

A. Ofrecer formación y concienciar en seguridad a las personas. Las personas suelen considerarse como el elemento más débil en la seguridad de la información. Los errores humanos están en el origen de un importante número de incidentes.

Por ello, es fundamental tener un plan de concienciación y formación en seguridad para el personal de la organización, incluidos los puestos de alta dirección que no pueden ser ajenos a estos riesgos. Son multitud los aspectos que deben abordarse a lo largo de dicho plan, pero debemos destacar todas aquellas acciones encaminadas a detectar campañas de *'phising'* como un aspecto prioritario, dado que es el principal vector de entrada utilizado para otro tipo de ataques (robo de credenciales, *'ransomware'*, etc.). Conviene concienciar al personal sobre las medidas mínimas: desconfiar de correos de contenido sospechoso (aunque se conozca al remitente), no abrir los adjuntos y no acceder a los enlaces incluidos en los correos.

B. Desplegar Microclaudia, solución **contra *'ransomware'*** del Centro Criptológico Nacional (CCN) **gratuita** para organismos públicos, en todos los equipos (https://www.ccn-cert.cni.es/soluciones-seguridad/microclaudia.html).

C. Desplegar y mantener Antivirus/EDR (*'endpoint detection and response'*) en los equipos de usuarios. Es una medida de protección básica. La mayoría de organismos cuentan ya con soluciones antivirus. No obstante, si es posible, se recomienda soluciones más avanzadas, tipo EDR, basados en tecnologías que monitorizan y evalúan todas las actividades de los equipos finales y ofrecen una mejor protección de los tradicionales antivirus.

En cualquier caso, el despliegue de estas soluciones no es suficiente. Para que la medida sea eficaz es necesario una labor continua de gestión y mantenimiento asegurándose que en cada equipo a proteger, la aplicación se encuentra en ejecución, actualizada y configurada según las necesidades de uso específicas de cada organización. Igualmente importante es que la organización tenga la capacidad suficiente de monitorizar y atender con prontitud las alarmas generadas por la aplicación.

Como complemento de esta medida, puede resultar muy apropiado el despliegue de cortafuegos de prestaciones avanzadas (NGFW) que complementan la protección ofrecidas

por las soluciones de antivirus y EDR, así como de filtros de protección contra correos no deseados (filtros anti-spam).

D. Disponer de políticas de acceso restrictivas. Uno de los principales vectores de ataque es el robo de credenciales de acceso (habitualmente un primer paso de ataques más complejos y peligrosos). Disponer de políticas de control de acceso restrictivas, donde los permisos se otorgan exclusivamente a los recursos imprescindibles para las tareas encomendadas ayuda a minimizar el impacto en el organización en el caso de robo de credenciales. La validez de los permisos concedidos debe ser revisada periódicamente.

Por otra parte, disponer de doble factor de autenticación en los servicios accesibles remotamente, así como para los usuarios con privilegios de administración, reduce significativamente la eficacia del robo de credenciales.

E. Mantener actualizadas los sistemas operativos y las aplicaciones. Muchas de las circunstancias indeseables para la seguridad de los tratamientos derivan de la falta de actualización del software empleado. Un política de análisis de vulnerabilidades y de actualización constante resulta esencial.

La prioridad debe establecerse para aquellos servicios que se encuentren expuestos en internet ya que son los que tendrán una mayor probabilidad de ser atacados, sin olvidar, por supuesto, el resto de servicios y aplicaciones que también pueden ser objeto de ataques.

F. Disponer de copias de seguridad operativas y verificadas periódicamente. No es suficiente con tener algún sistema de copias de seguridad. Es crítico para la pronta restauración del servicio en caso de incidente, que dichas copias se almacenen de forma segurda y que al menos una de las copia tenga una separación completa de la red del organismo. Así será inaccesible por cualquier actividad o código dañino que se produzca.

Igualmente crítico es que se monitoricen diariamente la correcta realización de las mismas y que se realicen pruebas de recuperación de información desde las copias de seguridad de forma periódica.

G. Aplicar la diligencia debida en la contratación de encargados de tratamiento. Los responsables del tratamiento tienen que velar por la efectiva puesta en práctica de las medidas de seguridad. No es posible delegar dicha responsabilidad. Así, aún cuando haya un encargado del tratamiento (es muchos caso con mayor especialización técnica), el responsable tiene que asegurarse de que el encargado está en condiciones de cumplir sus obligaciones en materia de protección de datos y hacer un seguimiento periódico, apoyándose en el responsable de seguridad.

5.2 Dispositivo perdido, robado o desechado

En este ámbito caben aplicar dos tipos de medidas, una orientada a evitar el suceso y otro, más importante si cabe, a minimizar el impacto del mismo.

Por el lado de evitar que ocurra, se recomienda emplear mecanismos de anclaje de los equipos portátiles en los puestos de trabajo y la custodia bajo llave de cualquier dispositivo empleado. Igualmente, pueden realizarse campañas de concienciación entre el personal.

Por el lado de la minimización existen técnicas sencillas de desplegar y robustas que minimizan en gran medida el impacto en caso de ocurrencia. Entre ellas destacamos:

- Emplear cifrado de discos duros, smartphones y memorias USB (pen-drive). En la aplicación de estas medidas no puede olvidarse custodiar de forma segura la clave de recuperación (descifrado).
- Utilizar claves robustas de acceso para impedir ataques de fuerza bruta.
- En el caso concreto de los sistemas operativos, se evitará mostrar el nombre del último usuario que inició sesión en el equipo.
- En el caso de dispositivos que se conecten a la red, habilitar la funcionalidad de bloqueo/eliminación remota.

En cualquier caso, como recomendación general, lo adecuado es restringir al mínimo imprescindible los casos en los que se empleen dispositivos portátiles que contengan datos personales y disponer siempre de una copia de seguridad en lugar seguro de los mismos.

5.3 Datos enviados/mostrados por error (postal o electrónicamente)

Este tipo de incidentes no son sencillos de erradicar ya que se deben a errores humanos principalmente. Al cabo del día son muchos los correos (o envíos postales) que una persona puede llegar a realizar. En cualquier caso las siguientes pautas pueden contribuir a reducir la ocurrencia y el impacto de los mismos:

- Utilizar listas de distribución con acceso restringido a un número limitado de personas. Concienciar a dichas personas de la especial precaución que se debe adoptar en su uso.
- Establecer procedimientos en los que el envío de correos especialmente sensibles requiera la revisión previa de otra persona.

- Enviar la documentación cifrada por correo electrónico y utilizar otra vía para proporcionar la clave de acceso
- Disponer de sistemas de información que faciliten la puesta disposición de la información por otras vía y que caso de necesidad de envío de correo, los automaticen y contengan reglas de validación automáticas.
- Realizar campañas periódicas de concienciación sobre este tipo de errores.
- Establecer mecanismos de bloqueo de pantalla automático transcurrido un cierto tiempo sin actividad.
- Instalar en los equipos filtros de pantalla de privacidad para evitar la “piratería visual”.

5.4 Comunicación, difusión o publicación indebida de datos

Este tipo de incidentes e incumplimientos pueden minimizarse atendiendo a las siguientes recomendaciones:

- Revisar (o redactar) una política de protección de datos así como los procedimientos específicos que la desarrollen. En ellos se especificarán para cada tratamiento de la organización, los casos en que sea posible comunicar o publicar determinados datos personales así como las condiciones en las que puede realizarse. Se recomienda adoptar un enfoque de “lista blanca”, eliminando por defecto cualquier dato que no esté incluido en los permitidos, de acuerdo con el principio de minimización establecido en el RGPD.
- Estudiar situaciones en las que no sea necesaria la difusión o publicación de datos personales. Para ello, se recomienda establecer un procedimiento de anonimización de la información en la organización.
- Establecer y divulgar buenas prácticas en el uso de sistemas de correo electrónico y de mensajería instantánea por parte del personal.
- Determinar las situaciones concretas en las que no sea posible llevar a cabo la comunicación o difusión sin haber recabado previamente el consentimiento del interesado.
- Realizar sesiones formativas sobre sobre las normas y procedimientos establecidos y periódicamente realizar campañas de concienciación.

- Mantener una actitud proactiva de revisión periódica de los datos comunicados o publicados para detectar de forma anticipada posibles fallos en la ejecución de los procedimientos.

5.5 Acceso indebido a historia clínica

La principal recomendación a este respecto es la de reforzar las labores de **concienciación y formación** en el acceso y utilización de los datos que se manejan en la historia clínica de los pacientes. Por un lado, todo el personal debe conocer y asumir que los datos tratados son propiedad de las personas a las que atienden y que sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.

Cabe destacar como recurso formativo la Guía para profesionales del sector sanitario de la Agencia Española de Protección de Datos (AEPD)[2].

5.6 Videovigilancia incumpliendo la normativa

La instalación de videocámaras responde a una exigencia de garantía de seguridad y beneficio en la convivencia pacífica ciudadana. La normativa aplicable difiere en atención al ámbito en el que se vaya a desarrollar la vigilancia. La instalación de sistemas de videovigilancia y la captación de imágenes por los particulares y empresas en el ámbito de aplicación RGPD con fines de seguridad (no en el ámbito privado, ya que si la cámara se instala dentro de la propia vivienda sin enfocar fuera no se le aplicaría ninguna normativa) se regula principalmente en el artículo 22 de la LOPDGDD.

Si la finalidad fuera el control de los trabajadores, tendría que tenerse en cuenta lo establecido en el artículo 89 de la LOPDGDD.

La videovigilancia en espacios públicos con fines penales y de prevención de amenazas a la seguridad por autoridades competentes como Fuerzas y Cuerpos de Seguridad , Fiscalía o Tribunales se rige por la Ley Orgánica 7/2021, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. En todo aquello que no se oponga a esta norma, se aplicará la Ley Orgánica 4/1997, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos y su normativa de desarrollo.

La videovigilancia de tráfico se regirá también por lo dispuesto en el Real Decreto Legislativo 6/2015, por el que se aprueba el texto refundido de la Ley sobre Tráfico, Circulación

2 https://www.aepd.es/es/documento/guia-profesionales-sector-sanitario.pdf

de Vehículos a Motor y Seguridad Vial, relativa a los sistemas destinados al control de la disciplina en el tráfico.

El tratamiento de datos personales obtenidos por estos sistemas se regularán por la referida normativa. En este sentido, se recomienda:

• Tener en cuenta que las cámaras solo pueden captar espacios particulares. En caso de alcanzar a la vía pública, solo la parte imprescindible para garantizar la seguridad.

• El respeto al plazo máximo de conservación de las imágenes, así como su consecuente eliminación tras su finalización, salvo que estén relacionadas con infracciones penales o administrativas en materia de seguridad pública o una investigación policial en curso, que deberán ser puestas inmediatamente en disposición de la autoridad administrativa o judicial competente.

• La atención a los principios reguladores de los tratamientos de datos de personales, en especial su licitud y confidencialidad.

• Especial atención al deber de informar debidamente en lugar suficientemente visible, identificando la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en el RGPD.

• Especial atención al principio de proporcionalidad en la adopción de la autorización para la instalación de los dispositivos, elaborando un análisis ponderado de la finalidad que motiva su adopción, el carácter intrusivo de la medida, y su adecuación.

• Cuando la instalación de las cámaras suponga una vigilancia sistemática y a gran escala de un espacio de acceso público, requerirá la realización de una evaluación de impacto relativa a la protección de datos con carácter previo a la instalación de las la mismas, atendiendo a la naturaleza, alcance, contexto, fines y el riesgo para los derechos y libertades de las personas físicas del tratamiento.

Finalmente, sugerimos acudir a la Guía sobre el uso de videocámaras para seguridad y otras finalidades de la AEPD para obtener más información sobre la materia[3].

5.7 Tratamiento indebido de datos

Para intentar evitar estas situaciones, se recomienda:

- Lanzar una tarea de descubrimiento de tratamientos en la organización y asegurar que ninguno queda fuera del inventario de actividades de tratamiento.

3 https://www.aepd.es/es/documento/guia-videovigilancia.pdf

- Revisar y actualizar el inventario de actividades de tratamiento de acuerdo a lo establecido en el artículo 30 RGPD y artículo 31 LOPDGDD. Se pondrá especial atención a la finalidad, a la identificación y justificación de la base legitimadora del tratamiento, así como las comunicaciones de datos personales previstas. Esta labor debe realizarse a conciencia, con el asesoramiento y supervisión del DPD y no ser consideradas como un mero formalismo.
- Contrastar la información obtenida tras dicha revisión con la que se proporciona a los interesados en el momento de la recogida de datos. Además de proporcionar la mínima requerida en los artículo 13 y 14 RGPD, debe revisarse que la información se traslada mediante cláusulas de información concisas, claras e inteligibles, que sean fácilmente accesibles y que permitan a los interesados comprender el alcance del tratamiento de sus datos, los riesgos a los que pueden verse expuestos, así como el modo de hacer valer sus derechos en materia de protección de datos[4].
- Revisar los casos en los que la base legitimadora es el consentimiento y contrastar su validez. En ese caso, comprobar que se cumplen todos los requisitos establecidos en el artículo 7 RGPD. El responsable del tratamiento debe ser capaz de demostrar que se ha recabado. Se prestará especial atención a los casos en los que se traten datos de categorías especiales (artículo 9 RGPD), se adopten decisiones automatizadas (artículo 22 RGPD) o se realicen transferencias internacionales (artículo 49 RGPD). En estos casos, el consentimiento, de ser necesario, debe ser explícito. Pueden consultarse las Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 del Comité Europeo de Protección de Datos para entender los requisitos que debe satisfacer dicho consentimiento explícito. Dichas directrices ofrecen igualmente un análisis exhaustivo del concepto y una orientación práctica para obtener y demostrar un consentimiento válido.[5]

5.8 Carencia de Delegado de Protección de Datos

En este supuesto, la recomendación, no se limita a cumplir con el formalismo de realizar la designación del DPD y comunicarlo a la autoridad de control, con independencia de que ambas cosas han de realizarse. Para que la medida sea realmente eficaz y aporte valor a la organización, el nombramiento debe atender a los criterios y requisitos establecidos en los artículos 37 a 39 RGPD y en los artículos 34 a 37 LODPGDD. A modo de resumen no exhaustivo, destacamos las siguientes pautas generales del DPD nombrado, que

4 https://www.aepd.es/es/documento/guia-privacidad-desde-diseno.pdf(Apartado I.6)

5 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf

se verán moduladas en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados:

- Disponer de conocimientos en materia de protección de datos, así como de los procesos de la organización en la que presta servicio.
- Contar con independencia en sus actuaciones como DPD, con interlocución al más alto nivel jerárquico del responsable de tratamiento donde preste sus servicios y sin presentar conflictos de intereses que influyan en su función como DPD. Como norma general, dichos conflictos tienen lugar en los puestos de alta dirección pero también otros cargos inferiores si tales cargos o puestos llevan a la determinación de los fines y medios del tratamiento[6].
- Contar con los recursos humanos, económicos y formativos suficientes para el desempeño de sus funciones en un adecuado régimen de dedicación.
- Disponer, en el ejercicio de sus funciones, de acceso a los datos personales y procesos de tratamiento.
- Ser debidamente publicitado, tanto a nivel interno como a nivel externo a la organización.

5.9 Uso de datos para finalidades incompatibles

Como se ha visto anteriormente, se corresponde con situaciones en la que los reclamantes consideran que los datos son tratados para otros fines distintos para los que fueron recogidos. Las recomendaciones se orientan en establecer normas y procedimientos que proporcionen una información clara a las personas sobre dichos fines y en todo caso eviten los tratamientos que realmente puedan ser incompatibles.

- Mantener actualizado el Inventario de Actividades de Tratamiento, con una descripción clara y completa de la finalidad de los mismos y de su base legal, incidiendo, en su caso, en la condición que levanta la prohibición del tratamiento de categorías especiales de datos (recordemos además, la obligación de publicar dicho inventario en el caso del sector público).
- Concienciar y formar al personal en el principio de limitación de la finalidad (artículo 5.1.b) RGPD).

6 Directrices sobre los delegados de protección de datos (DPD) del GT29. https://www.aepd.es/es/media/criterios/wp243rev01-es.pdf

- Establecer un procedimiento interno por el que si surge la necesidad de realizar un tratamiento con una finalidad distinta de las contempladas en el Inventario de Actividades de Tratamiento, se exija realizar y documentar el "test de compatibilidad" recogido en el artículo 6.4 RGPD. Esta actividad se realizará con el asesoramiento del DPD. Si es necesario, actualizar el Inventario e informar a los interesados oportunamente.
- En caso de duda sobre la compatibilidad, se actuará con la máxima cautela y no se iniciará el tratamiento propuesto hasta que puedan identificarse alternativas compatibles con el RGPD.

6. TABLA RESUMEN DE RECOMENDACIONES

La tabla siguiente resume las principales recomendaciones realizadas en el documento.

CAUSAS	RECOMENDACIONES
CIBERINCIDENTE: HACKING, MALWARE O PHISHING ---------- MEDIDAS TÉCNICAS	**Certificación ENS.** **Concretas:** - Concienciación y formación en seguridad TIC - microclaudia y EDR: Mantenimiento y monitorización continua - Control de acceso y autenticación por doble factor - Actualización del software - Copias de seguridad validadas - Contratación diligente de encargados del tratamiento
DISPOSITIVO PERDIDO, ROBADO O DESECHADO	- Evitar: dispositivos anti-robo, custodia bajo llave, concienciación - Mitigar impacto: cifrado, claves robustas, bloqueo/eliminación remota
DATOS ENVIADOS / MOSTRADOS POR ERROR (POSTAL O ELECTRÓNICAMENTE)	- Listas de distribución de uso restringido - Revisión por segundas personas - Envío de documentación cifrada y traslado de clave por vía alternativa - Automatización y verificación de envíos mediante sistemas de información - Campañas de concienciación sobre errores
COMUNICACIÓN, DIFUSIÓN O PUBLICACIÓN INDEBIDA DE DATOS	- Política de protección de datos y procedimientos. Enfoque de "lista blanca" - Publicar sólo de forma anonimizada. Crear procedimiento - Buenas prácticas para el uso de correo y mensajería instantánea - Verificar si es necesario el consentimiento antes de comunicar/publicar - Formación y concienciación - Revisión periódica de los contenidos publicados
ACCESO INDEBIDO A HISTORIA CLÍNICA	- Concienciación y formación en el correcto uso por parte del personal sanitario
VIDEOVIGILANCIA INCUMPLIENDO NORMATIVA	- Estudio detallado de la necesidad. - Verificación del cumplimiento según las Guías publicadas por la AEPD
TRATAMIENTO INDEBIDO DE DATOS O SIN EL CONSENTIMIENTO DEBIDO	- Descubrimiento de todos los tratamientos de la organización - Revisión y actualización del inventario de actividades de tratamiento. Foco en finalidad, base legitimadora y comunicaciones - Revisión del fondo y forma de la información ofrecida a los interesados - Verificación de los requisitos necesarios para consentimiento válido. Atención a los consentimientos explícitos
CARENCIA DPD	- Proceder a su nombramiento y comunicación a la autoridad de control - Evitar un mero cumplimiento formal - Conocimientos en protección de datos y en la organización - Independencia y sin conflicto de intereses - Disponer de recursos suficientes
USO DE DATOS PARA FINALIDADES INCOMPATIBLES	- Revisión y actualización del inventario de actividades de tratamiento - Establecer procedimiento interno para "test de compatibilidad". - No realizar en caso de dudas

Tabla 3. Resumen de recomendaciones

7. ANEXO. METODOLOGÍA EMPLEADA EN EL ANÁLISIS

Para el análisis se ha partido de la información de reclamaciones y de brechas de datos personales disponibles en el Consejo a fecha de 20 de marzo de 2023.

En concreto, se han estudiado 111 de brechas de datos personales y 421 reclamaciones. Debe tenerse en cuenta que no se incluyen aquellas que reclamaciones relacionadas con la solicitud de ejercicio de los derechos reconocidos en los artículos 15 a 22 de RGPD, dado que están principalmente relacionadas con procesos internos de gestión de las organizaciones y podrán ser objeto de un análisis específico).

CONCEPTO	Número
BRECHAS DE DATOS PERSONALES	**111**
RECLAMACIONES POR OTRAS VULNERACIONES	**421**

Tabla 4. Número de brechas y reclamaciones analizadas

Para determinar las causas de cada una de ellas, se han empleado distintos conceptos, cada uno más adaptado a sus características particulares de las brechas y reclamaciones. Para las brechas de datos personales se ha considerado como elemento calificador el tipo de incidente. Para el caso de las reclamaciones, se ha tomado el concepto de materia y motivo extraídos de las descripciones que las personas realizan en las mismas.

De esta forma, una vez determinadas las brechas y reclamaciones a clasificar así como los conceptos sobre los que clasificar, se procede a la asignación caso por caso del tipo de incidente o motivo que le corresponda. Finalmente, se identificaron las tipologías más frecuentes, generándose una lista reducida con las causas más frecuentes. En el caso de brechas de datos personales, 4 tipos de incidente permiten resumir el 80% de las mismas y para el caso de reclamaciones, empleando 9 motivos es posible explicar el origen del 75% de dichas reclamaciones.

En el caso de las brechas de datos personales se han tenido en consideración los siguientes tipos de incidentes:

TIPO INCIDENTE
INCIDENCIA TÉCNICA
DATOS PERSONALES MODIFICADOS / PERDIDOS / BORRADOS
ABUSO DE PRIVILEGIOS DE ACCESO
ENVÍO DE CORREO A MÚLTIPLES DESTINATARIOS SIN CCO
PUBLICACIÓN INDEBIDA
DATOS ENVIADOS / MOSTRADOS POR ERROR (POSTAL O ELECTRÓNICAMENTE)
REVELACIÓN INDEBIDA DE DATOS PERSONALES
DISPOSITIVO PERDIDO, ROBADO O DESECHADO
DOCUMENTACIÓN PAPEL PERDIDA, ROBADA O EN LOCALIZACIÓN INSEGURA O ELIMINADA INCORRECTAMENTE
CIBERINCIDENTE: HACKING, MALWARE O PHISHING

Tabla 5. Tipos de incidentes en brechas de datos personales

En el caso de las reclamaciones, se han tenido en consideración los siguientes motivos, agrupados a su vez en materias (determinados a partir de las descripciones de las reclamaciones). Para los fines de este análisis, sólo se tomará en consideración los motivos, a los efectos de no diversificar excesivamente las conclusiones y recomendaciones.

MATERIAS	MOTIVOS
PRINCIPIOS DEL TRATAMIENTO	CONSERVACIÓN DATOS MÁS TIEMPO DEL NECESARIO
	INEXACTITUD DE DATOS
	MINIMIZACIÓN DE DATOS (RECOGIDA, TRATAMIENTO O ACCESOS EXCESIVOS)
	USO DE DATOS PARA FINALIDADES INCOMPATIBLES
LICITUD DEL TRATAMIENTO	FALTA DE CONDICIÓN QUE LEGITIME EL TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS
	FALTA DE CONDICIÓN QUE LEGITIME LA LICITUD DEL TRATAMIENTO

	TRATAMIENTO SIN EL CONSENTIMIENTO DEBIDO
DERECHOS DEL INTERESADO	FALTA RESPUESTA A DERECHOS DEL INTERESADO
	RESPUESTA INCORRECTA A DERECHOS DEL INTERESADO
MEDIDAS ORGANIZATIVAS	CARENCIA DPD
	CARENCIAS EN CONTRATO TRATAMIENTO
	CARENCIAS EN INFORMACIÓN A INTERESADOS
	CARENCIAS EN LA OBTENCIÓN DEL CONSENTIMIENTO
	FALTA PUBLICACIÓN INVENTARIO RAT
MEDIDAS TÉCNICAS	CARENCIA MEDIDAS SEGURIDAD
	CARENCIAS EN ANÁLISIS DE RIESGOS
	CARENCIAS EN EVALUACIÓN DE IMPACTO SOBRE PD
	QUIEBRA MEDIDAS SEGURIDAD
	USO DE DATOS REALES EN ENTORNOS DE PRUEBA
TRATAMIENTO INDEBIDO DE DATOS	ACCESO INDEBIDO A HISTORIA CLÍNICA
	CARENCIAS EN SISTEMAS DE GEOLOCALIZACIÓN
	COMUNICACIÓN INDEBIDA DE DATOS
	COMUNICACIÓN INDEBIDA DE DATOS DE RECLAMANTES O SOLICITANTES
	CONTROL DE TEMPERATURA
	CORREO ELECTRÓNICO SIN USO COPIA OCULTA
	DIFUSIÓN O PUBLICACIÓN INDEBIDA DE DATOS
	DIVULGACIÓN O USO INDEBIDOS DE CSV
	GRABACIÓN DE REUNIONES O SESIONES FORMATIVAS
	NOTIFICACIONES INCORRECTAS
	PUBLICACIÓN COMPLETA DNI EN NOTIFICACIONES (DA 7ª)

	TRATAMIENTO INDEBIDO DE DATOS
	TRATAMIENTOS BIOMÉTRICOS
	TRATAMIENTOS DE DATOS EN LA NUBE
	USO INADECUADO DE SISTEMAS DE MENSAJERÍA
	VIDEOVIGILANCIA INCUMPLIENDO NORMATIVA
ENTORNO WEB	CARENCIAS EN POLÍTICAS DE PRIVACIDAD
	INCORRECTAS POLÍTICAS SOBRE COOKIES
INCUMPLIMIENTO RESOLUCIONES O FALTA COLABORACIÓN	FALTA COLABORACIÓN AUT. CONTROL
	INCUMPLIMIENTO RESOLUCIONES AUT. CONTROL
INCUMPLIMIENTO GENÉRICO	INCUMPLIMIENTO GENÉRICO DE LA NORMATIVA

Tabla 6. Tipos de materias y motivos en reclamaciones (extraído del contenido de reclamaciones)